Cassandra Crossing/ Tails per tutti

(266) - E tutti per Tails. Un sistema operativo per paranoici, per amanti della privacy, per chi è costretto a vivere in incognito.

Cassandra Crossing/ Tails per tutti

(266) - E tutti per Tails. Un sistema operativo per paranoici, per amanti della privacy, per chi è costretto a vivere in incognito.

Figure 1:

23 novembre 2012—Gli habitué di Cassandra hanno già sentito parlare di Tails, una distribuzione GNU/Linux live basata su Debian che include tutti i normali servizi di Rete, installati però in modalità paranoica per funzionare solo attraverso la rete Tor, quindi usando sempre connessioni criptate.

Si tratta di uno strumento inizialmente pensato per un utilizzo di nicchia, come un giornalista in zona di guerra o un dissidente, che sono posti davanti alla scelta se usare queste tecniche, stare zitti o finire assai male.
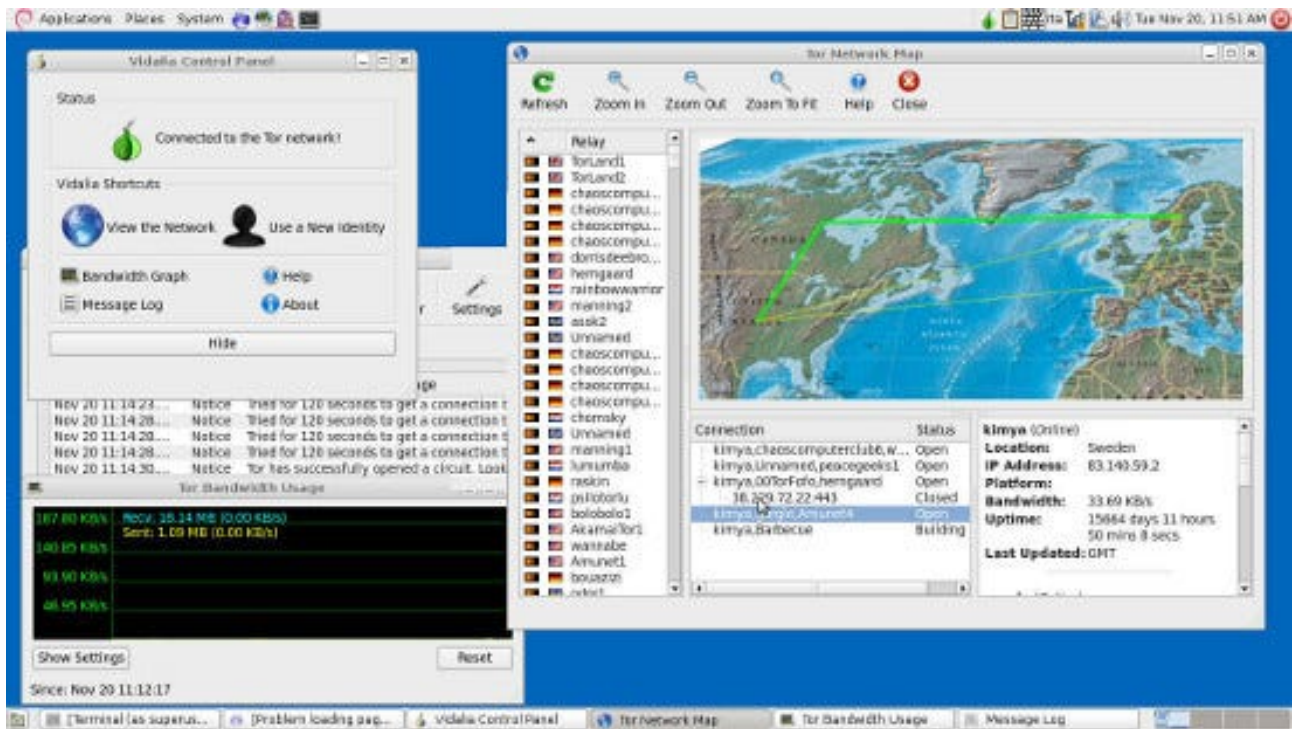
Figure 2:

Tails nasce infatti dalla produttiva fusione di due progetti simili (Amnesia e Incognito) da cui la sigla The Amnesic Incognito Live System (ed il logo che rapresenta la coda di un gatto), pensati per un impiego della Rete dove non esistano alternative oltre l'espulsione, il carcere o la morte.

È chiaro che l'usabilità di un sistema operativo live cd, che non memorizza i bookmark, gli account di posta, le chiavi pgp, i nickname delle chat e così via, è, per forzata scelta progettuale, molto bassa.

D'altra parte non è infettabile da virus o, peggio, da trojan, e non lascia tracce sul computer che lo ospita, perché non solo non tocca nemmeno il disco ma cancella anche la RAM alla fine della sessione. Cassandra ha sempre cercato di promuovere un utilizzo il più esteso possibile della crittografia nelle comunicazioni elettroniche, al fine di contrastare le derive del tecnocontrollo sociale che in tutti i paesi occidentali (in questa sede sarebbe azzardato parlare di "democrazie occidentali"), sta conoscendo una crescita esponenziale.

Ed eccoci al punto. Si dà il caso che una delle caratteristiche dell'ultima release di Tails, unita alla onnipresenza delle chiavette USB ed alla capacità di tutti i portatili moderni di eseguire da chiavetta USB e senza alchimie il boot di un sistema operativo, segni un incremento gigantesco in termini proprio di usabilità. Questo rende possibile l'uso di Tails anche alle persone normali, che non rischiano la vita ma sono un po' paranoiche o più semplicemente tengono molto alla propria privacy.

Infatti la versione 0.14 di Tails, distribuita nel solito formato di immagine ISO da masterizzare su un cd (anzi, per motivi di spazio ormai su un DVD), possiede nell'apposito menù "Tails" due programmi di utilità che le permettono di copiare se stessa su una chiavetta USB, e di abilitare selettivamente la persistenza delle informazioni che si desiderano conservare su una partizione criptata con LUKS.

Questo si ottiene con due elementari operazioni che è più lungo descrivere che eseguire (bastano due minuti due) e che comunque possono essere eseguite una tantum da una persona fidata che

inizializzi la chiavetta per vostro conto.
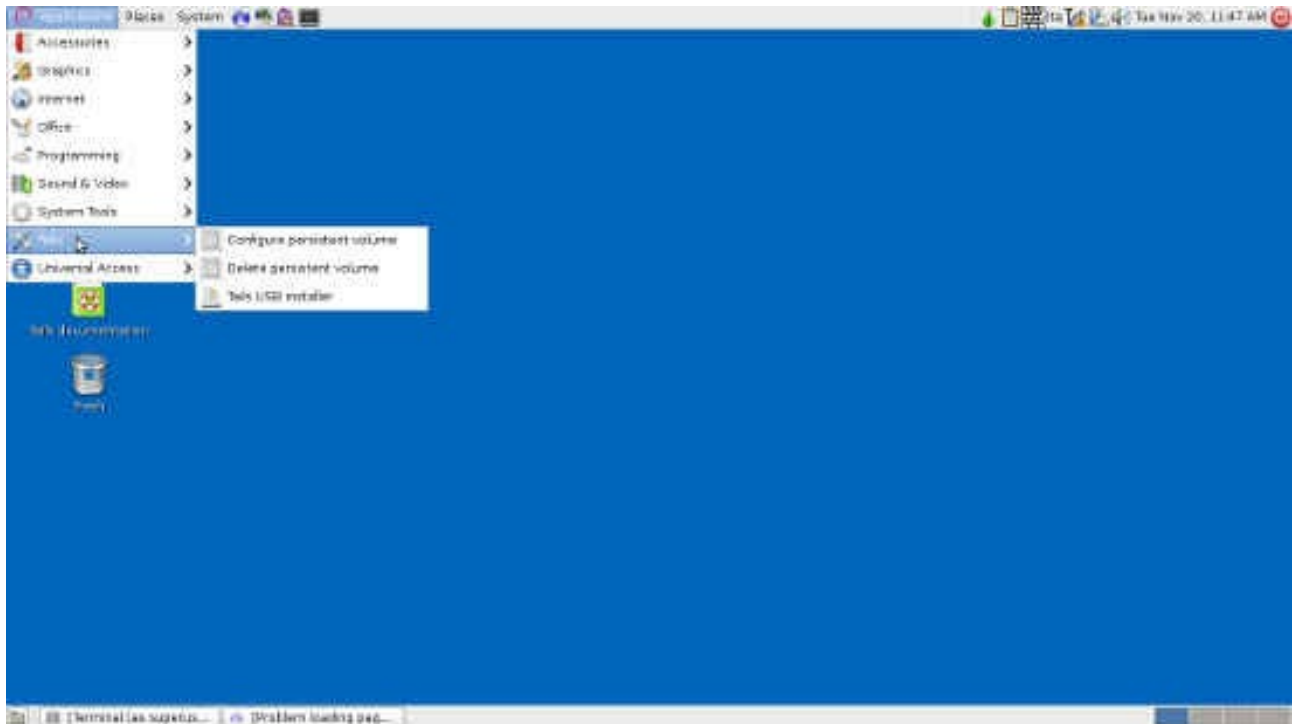
Figure 3:

L'utente può scegliere su quale tipo di informazioni abilitare la persistenza, dal solo keyring delle chiavi pubbliche e private fino ai settaggi ed i bookmark del browser, interi file o folder, o su tutta la directory home.Questo rende possibile gestire con Tails tutti i normali scambi di informazioni in Rete (mail, navigazione, chat ed altro) in forma anonima via Tor, e di conservare le informazioni riservate, sia esistenti che generate dalla navigazione, in modalità protetta.
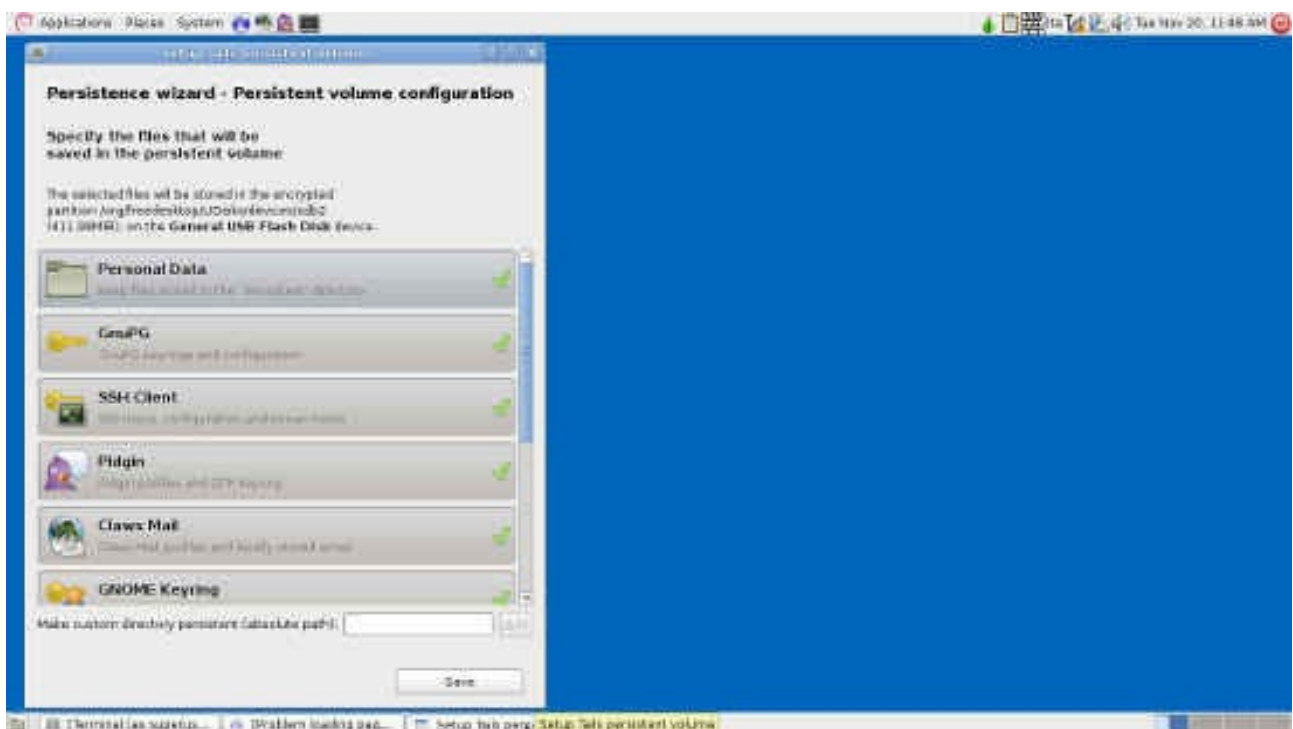
Figure 4:

Permangono ovviamente le limitazioni della rete Tor in termini di velocità, che però diventano trascurabili nel momento in cui non si fanno navigazioni su portali pieni di pubblicità ed effetti speciali, ma su siti più amichevoli e normali.

Un'altra utile caratteristica, che è stata a lungo dibattuta dagli sviluppatori prima del suo inserimento, permette anche, dopo aver ripetutamente diffidato l'utente sui pericoli connessi con il suo uso, di lanciare ove fosse necessario un browser separato nella "anomala modalità normale", cioè al di fuori della Rete Tor: è una piccola diminuzione di sicurezza ma un altro grosso guadagno in termini di usabilità.

Un'ulteriore caratteristica che dimostra il taglio "emergenziale" di Tails la potete scoprire se durante una sessione staccate la chiavetta USB: il sistema se ne accorge ed esegue automaticamente l'immediata cancellazione della RAM e spenge il computer.

Non fate questa prova con la persistenza abilitata perché potreste ovviamente danneggiare la partizione criptata.

Gratis arriva poi la possibilità di usare la chiavetta USB contenente Tails come semplice chiavetta criptata: le principali distribuzioni di GNU/Linux implementano ormai l'automount di partizioni criptate quindi, dopo aver bootstrappato il vostro normale sistema operativo, basta inserire la chiavetta contente Tails con persistenza abilitata, ed il sistema vi offrirà automaticamente la possibilità di montarla come semplice chiavetta criptata.
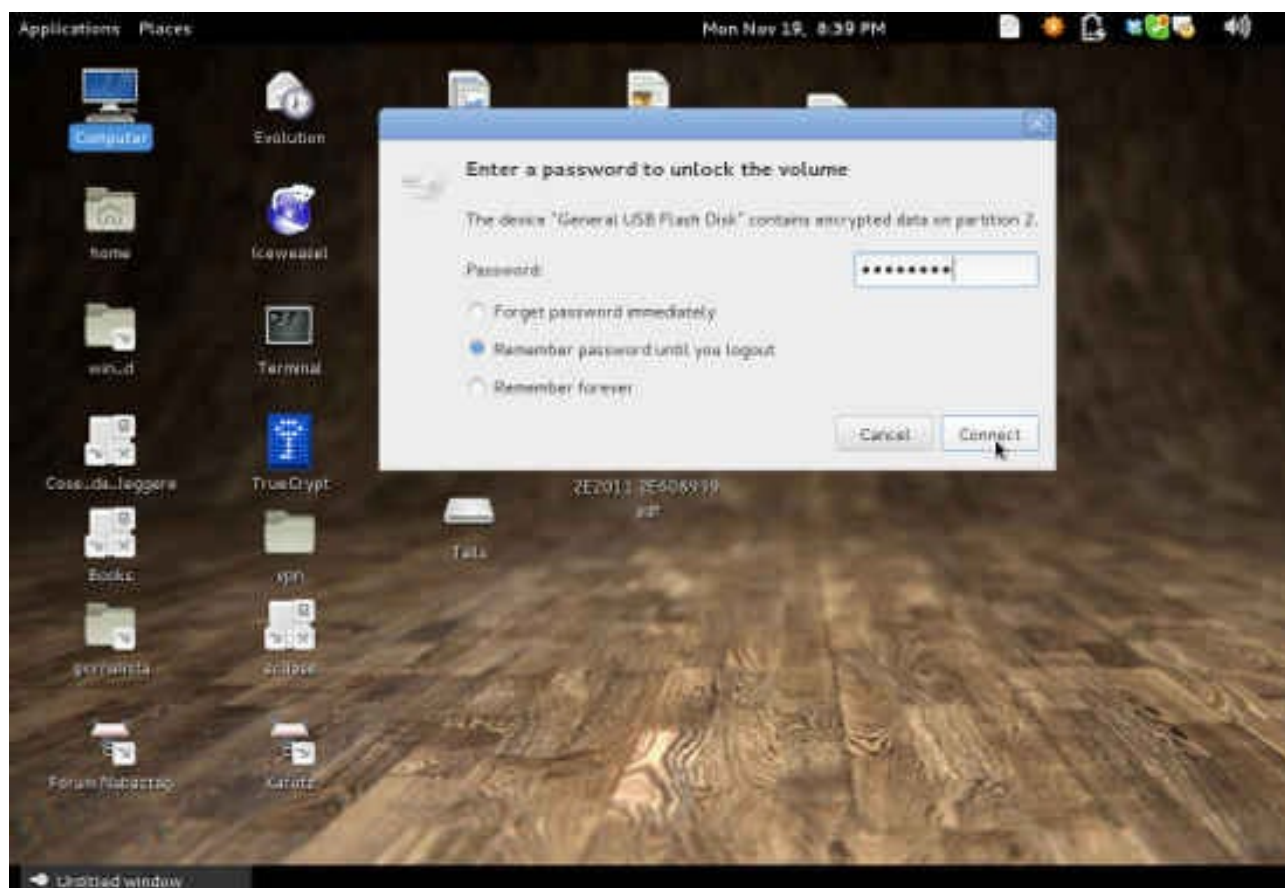
Figure 5:

E cosa dire a chi è costretto ad usare altri noti ma non liberi sistemi operativi? Primo che, anche se non è colpa loro, la loro vita sarà un po' meno comoda (e invece, se lo fanno volontariamente,

che se lo meritano). Nulla impedirà ovviamente di bootstrappare Tails, ma caratteristiche comode come l'automount della partizione criptata non saranno disponibili, salvo smanettamenti la cui descrizione appesantirebbe questa sintetica introduzione.

Nel caso la cosa potesse invogliarli ad usare Tails, merita citare che può essere bootstrappata in una modalità "mascherata", in cui l'aspetto tipico dell'interfaccia di GNU/Linux (si chiama Gnome, giusto per informazione) viene sostituita dall'aspetto "collinoso" di un diffuso anche se vecchiotto sistema operativo proprietario.

A consolazione e beneficio di chi abbia comunque bisogno di usare anche sistemi operativi non liberi Tails, con un approccio pragmatico, include anche Truecrypt, che deve semplicemente essere abilitato con una semplice scelta durante il boot e che, essendo disponibile su tutti i principali sistemi operativi, permette di usare una partizione criptata formattata Truecrypt in modalità cross-platform.

Dulcis in fundo, Tails permette da tempo di installare al volo applicazioni che non siano già presenti nella distribuzione base: questo obbligava però a scaricare ogni volta le stesse applicazioni ad ogni boot.

La persistenza può essere oggi abilitata anche sulle liste dei pacchetti e sui pacchetti stessi, evitando così di dover aggiornare e scaricare pacchetti ad ogni utilizzo.

Non rimane che da fornire l'indirizzo del sito del progetto Tails, il link diretto da cui scaricare l'immagine ISO (usate il link bittorrent ove possibile per non rubare risorse al sito stesso) ed infine l'indirizzo della mailing list degli annunci di nuove versioni e di quella del gruppo di sviluppo.

Last, but not least, Cassandra fa l'usuale "chiamata alle armi": se siete in grado di contribuire allo sviluppo e ai test (questi ultimi molto importanti e complessi, particolarmente in questa fase dello sviluppo di Tails) siete caldamente invitati a prendere contatto con la lista degli sviluppatori (in inglese).

La collaborazione è possibile (e doverosa) anche per coloro che non sono in grado di programmare o amministrare sistemi GNU/Linux, ma che conoscono un po' di inglese: possono collaborare all'opera di internazionalizzazione di Tails che è attualmente in corso.

Si è infatti recentemente costituito uno microscopico gruppo di traduttori che si è assegnato l'ambizioso obbiettivo di realizzare la versione italiana sia di Tails che del sito. Cassandra sta parlando proprio di voi, quindi siete caldamente invitati a partecipare.

Gli interessati possono contattare la mailing list dedicata all'internazionalizzazione o direttamente chi preme i tasti per conto di Cassandra.

Enjoy.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on July 15, 2023.

Canonical link

Exported from Medium on August 27, 2025.